Lightweight Cryptography for IOT Devices: An Overview

Soham Vaidya,
Master of Science (Cyber Security) Student, Nanyang Technological University Singapore

Abstract

The rapid growth of IoT (Internet of Things) devices has revolutionized modern life, enabling intelligent solutions in urban planning, industrial automation, and healthcare. However, the limited memory, energy, and processing capabilities of these devices present significant challenges for traditional cryptography. Lightweight cryptography (LWC) has emerged as a vital solution, ensuring security within these constraints.

This work provides an overview of lightweight cryptography, highlighting its design principles, key algorithms like ASCON, PRESENT, and GIFT, and applications in IoT settings. ASCON, recognized as the NIST standard, exemplifies efficient authentication and encryption with minimal resource usage. LWC emphasizes resource optimization, efficiency, and simplicity through techniques like modular arithmetic and reduced computational complexity.

Applications span domains such as wearable technology, sensor networks, and smart homes. For instance, LWC protects real-time data in healthcare IoT devices and secures communication in smart city ecosystems. Future directions include developing quantum-resilient cryptography, enhancing defences against side-channel attacks, and advancing energy-efficient cryptographic systems. Collaboration between academia, industry, and standards bodies is crucial to achieving these goals.

In conclusion, lightweight cryptography plays a pivotal role in enabling secure, scalable solutions for billions of connected devices, driving secure digital transformation in resource-constrained environments.

Key words: *Lightweight Cryptography, IOT Devices, Design Principles, Applications*

Introduction

Modern lifestyles are being shaped by smart technologies and gadgets, such as the Internet of Things (IoT), as computers becomes more and more integrated into daily life. Gartner projects that IoT will dominate a $58 billion market by 2025 [1]. IoT devices rely on real-time data collected from sensors and transmitted over networks, enabling users to act on this information based on their needs [2][3]. The term “Internet of Things” (IoT) refers to a network of devices that are interconnected which can communicate through wired or wireless transmission [4].

These devices range from simple sensors to complex machinery, all contributing to improved efficiency, accuracy, and economic benefits through data sharing. However, scalability presents a significant challenge due to the constrained resources of IoT devices, as billions of devices require secure, real-time communication. Lightweight cryptography offers scalable solutions by providing robust security without overburdening computational or energy resources. It is specifically designed to accommodate the limited processing power, memory, and battery life of IoT devices. Despite advancements in low-cost cryptography, research on ultra-lightweight ciphers remains limited [6]. These devices often handle sensitive information, necessitating strong defenses against malicious threats. Cryptographic techniques tailored to IoT constraints enable secure communication without imposing excessive demands on device performance [7].

The aim of this paper is to deliver an overview of lightweight cryptographic algorithms, focusing on their design principles, applications, and associated challenges. This paper also explores real-world implementations and future directions, including the integration of quantum-resistant cryptography.

Existing Lightweight Cryptography

- ASCON: Created in 2014 for hashing and authenticated encryption with associated data (AEAD), ASCON uses a 320-bit sponge architecture and supports 128-bit keys. Its efficient encryption and hashing make it ideal for IoT applications with minimal resource consumption. In 2023, NIST selected ASCON as the lightweight cryptography standard. For example, ASCON secures communications in smart factories by ensuring data confidentiality and integrity with low energy usage. It uses a 64-bit IV and a shared 128-bit secret key for encryption and decryption, which can be securely exchanged via key encapsulation or a safe channel.
- PRESENT: Developed in 2007, this lightweight block cipher is optimized for hardware efficiency. It uses a 64-bit block size, key sizes of 80 or 128 bits, and an SP-network structure over 31 rounds. Its 4-bit S-box ensures hardware optimization, making it suitable for low-power applications like RFID tags in supply chain management.
- Simon and SPECK: Designed by the NSA for low energy consumption, Simon is optimized for hardware, while SPECK is suited for software implementations. These ciphers secure data transmission in IoT environments, such as smart cities, with minimal energy usage.
- GIFT: Introduced in 2017 as an improvement over PRESENT, GIFT uses a 64-bit block size, a 128-bit key, and an SPN structure with a 4-bit S-box. Its 28-round design balances efficiency and security while resisting linear and differential cryptanalysis, making it ideal for resource-constrained IoT devices.

These algorithms highlight lightweight cryptography's critical role in addressing IoT devices' resource constraints while ensuring robust security.

Comparison of Key Algorithms

The following table summarizes the key features of these algorithms:

Algorithm	Block Size (bits)	Key Size (bits)	Rounds	Structure	Speed	Resource Consumption	Known Vulnerabilities
ASCON	128	128	12	Sponge	Fast	Very Low	Selected by NIST for lightweight cryptography standardization [14]
PRESENT	64	80, 128	31	SPN	Medium	Low	Susceptible to linear and differential attacks on reduced rounds [7]
SPECK	32–128	64–256	22–34	ARX	Fast	Low	Vulnerable to differential cryptanalysis on reduced rounds [4]
Simon	32–128	64–256	32–72	Feistel	fast	Very Low	Vulnerable to differential cryptanalysis on reduced rounds [4]
GIFT	64	128	28	SPN	Fast	Very Low	Improved resistance; no practical attacks on full rounds reported [12]

Table 1: Lightweight Cryptography Algorithms and vulnerabilities

Challenges

Many issues arise for users and device owners as a result of the billions of connected devices running on different platforms, particularly as the emphasis moves from servers to sensors [6]. Concerns about privacy and security, compatibility, support and longevity requirements, technology limitations, and other issues are some of these difficulties [8]. Furthermore, IoT devices are highly vulnerable to a wide range of security threats [9]. As they interact directly with the physical environment to collect sensitive information or control variables, they become prime targets for attackers [10]. Such factors highlight the significance of cybersecurity in IoT systems, with essential requirements including confidentiality, integrity, availability, authentication and authorization, adherence to privacy and regulatory standards, and routine system updates [8]. Figure 4 illustrates the design trade-offs with respect to IoT devices.

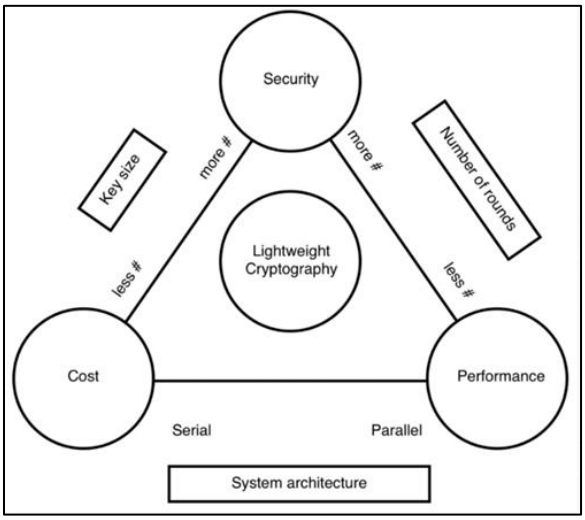

Figure 4: Lightweight cryptography: design trade-offs. [15]

It can also provide security for data stored or transmitted over networks. However, conventional cryptographic algorithms designed for PCs are unsuitable for IoT devices due to their significant resource requirements. Lightweight cryptography offers a solution by addressing these challenges and ensuring secure communication for resource-constrained IoT systems. These algorithms typically feature smaller block sizes of usually 32, 48, or 64 bits and key sizes less than 96. According to NIST guidelines, the minimum key length must be 112 bits. The primary challenges in implementing conventional cryptographic solutions in IoT devices are as follows [10]:

- **Limited memory (registers, RAM, ROM):** IoT devices often have constrained memory resources, typically just a few kilobytes, which restrict the implementation of complex cryptographic operations [5].
- **Reduced computing power:** IoT devices generally rely on less powerful CPUs compared to traditional computing systems, limiting their ability to perform resource-intensive cryptographic processes efficiently [5].
- **Small physical area for assembly:** The compact nature of IoT devices limits the available space for integrating cryptographic hardware, necessitating lightweight solutions that can fit these constraints [5].
- **Low battery power (or no battery):** Many IoT devices are battery-powered or operate without a battery. Energy efficiency is critical, as traditional cryptographic algorithms can drain power quickly, reducing device lifespan [5].
- **Real-time response requirements:** IoT systems often demand real-time data processing and communication. Conventional cryptographic operations can introduce delays, hindering the timely responses required by IoT applications [5].

To address these issues, lightweight cryptographic algorithms must be designed and implemented to meet the specific limitations of IoT devices effectively.

Applying conventional cryptographic standards to such IoT devices, particularly RFIDs and sensors, is impractical due to their constrained performance capabilities [6]. Lightweight cryptography effectively addresses these limitations by introducing features tailored to IoT environments, such as reduced memory requirements, lower computational demands, minimal energy consumption, and the ability to deliver real-time responses even on resource-constrained platforms [6].

Applications of Lightweight Cryptography

Lightweight cryptography is crucial in safeguarding resource-constrained devices across various domains. Its application is particularly significant in sensor networks, healthcare, automotive systems, smart homes, and smart cities, where conventional cryptographic solutions may not be feasible due to computational and resource limitations.

Sensor Networks and IoT

The Internet of Things (IoT) ecosystem comprises devices such as wearables, smart home appliances, and industrial sensors that enable seamless communication and data exchange. These devices operate with limited computational and energy resources, necessitating efficient security mechanisms. Lightweight cryptographic algorithms, such as SIMON, SPECK, PICCOLO, and TWINE, address these needs by providing robust security with minimal computational overhead.

For example, in environmental monitoring, lightweight encryption secures data integrity and confidentiality in sensor networks while preserving battery life. Similarly, wearable health trackers use low-power cryptographic

techniques to protect sensitive user data without compromising battery performance. Adoption of such cryptographic solutions is essential for the broad acceptance of IoT technologies [17].

Healthcare Systems

The integration of IoT devices has revolutionized healthcare by enabling real-time monitoring of patients through sensors tracking pulse, blood pressure, glucose levels, and oxygen levels. Ensuring the security and privacy of transmitted data is critical in this domain. Lightweight algorithms like SIMON, SPECK, PICCOLO, PRESENT, and Midori are well-suited for healthcare applications due to their compact hardware and software implementations. These solutions enable secure communication in both wearable and implanted devices, balancing security and energy efficiency.

A survey on lightweight encryption methods in IoT-enabled healthcare highlights their ability to meet the dual demands of security and efficiency, facilitating real-time patient monitoring while maintaining data confidentiality [18].

Smart cities

Smart cities deploy a vast array of IoT devices to enhance urban living, requiring stringent security measures to ensure the confidentiality and integrity of the data they generate and exchange. Lightweight cryptographic techniques provide the necessary protection without straining the network infrastructure.

Studies on lightweight encryption methods for smart cities emphasize their ability to address security concerns in intelligent systems. Authenticated encryption algorithms like Ascon have been evaluated for AI-enabled IoT devices, demonstrating their effectiveness in securing communications without sacrificing efficiency [22][23].

Future Scope

Despite these advancements, further research is required in several key areas to enhance the resilience and practicality of lightweight cryptographic solutions:

- **Resistance to Side-Channel Attacks:** Lightweight cryptographic algorithms are often vulnerable to side-channel attacks due to their simplified structures. Addressing these vulnerabilities without significantly increasing computational overhead remains a challenge. Techniques such as noise addition, which masks side-channel signals with random noise, and masking, which divides sensitive data into multiple parts to prevent leakage, are being explored as potential solutions [36].
- **Energy-Efficient Designs:** Since many lightweight cryptography applications rely on battery-powered devices, optimizing energy usage while maintaining security is essential. Research continues to explore energy-efficient cryptographic primitives and protocols. For instance, strategies like leveraging sparsity in leakage traces for artificial noise generation have been proposed to minimize energy consumption while preserving security [37].
- **Quantum-Safe Lightweight Cryptography:** The emergence of quantum computing poses a significant threat to traditional cryptographic methods. Developing lightweight algorithms resistant to quantum attacks is an unresolved challenge requiring innovative approaches. NIST's efforts to establish post-quantum cryptography standards mark an important step, but ensuring these algorithms perform effectively on resource-constrained devices remains a significant research focus [30].

Overcoming these challenges is critical to developing secure and efficient cryptographic solutions that meet the demands of modern, resource-constrained environments. Collaborative efforts among researchers, industry stakeholders, and standardization bodies are necessary to advance lightweight cryptography and ensure its robustness against evolving security threats.

Conclusions

Lightweight cryptography is essential for secure and efficient communication in resource-constrained environments, particularly within the rapidly expanding IoT ecosystem. By addressing the limitations of small devices—such as low processing power, memory, and energy—it delivers critical security features like encryption, authentication, and data integrity without compromising performance. Its applications span sectors such as healthcare wearables, smart homes, automotive systems, and industrial IoT, making it a cornerstone of secure digital transformation.

However, implementing lightweight cryptography comes with challenges, including balancing security and efficiency, defending against side-channel attacks, and preparing for quantum computing threats. Establishing global standards and ensuring interoperability among diverse IoT devices are crucial for widespread adoption. Continued collaboration among academia, industry, and standardization bodies will drive the development of robust, scalable, and universally compatible cryptographic protocols, ensuring the long-term security of interconnected systems.

References

[1] V. A. Thakor, “Lightweight Cryptography for Resource Constrained IoT devices,” thesis, Sep. 2022. [Online]. Available: https://research.tees.ac.uk/ws/portalfiles/portal/49903399/Lightweight_Cryptography_for_Resource.pdf

[2] Ding, J., Nemati, M., Ranaweera, C., and Choi, J. IoT. Connectivity Technologies and Applications: A Survey. IEEE Access. 2020; 8: 67646-67673.

[3] Alfred Y. Network Security. Malaysia: Asia Pacific University; 2019. pp. 5-11.

[4] K. A. McKay, L. Bassham, M. S. Turan, and N. Mouha, “Report on lightweight cryptography,” Mar. 2017. doi: 10.6028/nist.ir.8114. Available: https://csrc.nist.gov/pubs/ir/8114/final

[5] “Lightweight Cryptography for IoT: A State-of-the-Art,” Arxiv. Available: https://arxiv.org/pdf/2006.13813

[6] G. Hatzivasilis, K. Fysarakis, I. Papaefstathiou, and C. Manifavas, “A review of lightweight block ciphers,” Journal of Cryptographic Engineering, vol. 8, no. 2, pp. 141–184, Apr. 2017, doi: 10.1007/s13389-017-0160-y. Available: https://doi.org/10.1007/s13389-017-0160-y

[7] A. Bogdanov et al., “PRESENT: An Ultra-Lightweight Block Cipher,” in Lecture notes in computer science, 2007, pp. 450–466. doi: 10.1007/978-3-540-74735-2_31. Available: https://doi.org/10.1007/978-3-540-74735-2_31

[8] “Description, Implementation and Performance/Security Analysis of ASCON128 V1.2.” https://www.researchgate.net/publication/376380176_Description_Implementation_and_PerformanceSecurity_Analysis_of_ASCON128_V12

[9] Wikipedia contributors, “PRESENT,” Wikipedia, Jan. 26, 2024. https://en.wikipedia.org/wiki/PRESENT

[10] A. Menezes, P.C. van Oorschot, and S. Vanstone. The Handbook of Applied Cryptography. CRC Press, 1996.

[11] A. Bogdanov et al., “PRESENT: An Ultra-Lightweight Block Cipher,” An Ultra-Lightweight Block Cipher, [Online]. Available: https://iacr.org/archive/ches2007/47270450/47270450.pdf

[12] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, “The SIMON and SPECK Families of Lightweight Block Ciphers,” IACR Cryptology ePrint Archive, Jun. 20, 2013. Available: https://eprint.iacr.org/2013/404

[13] S. Banik, S. K. Pandey, T. Peyrin, Y. Sasaki, S. M. Sim, and Y. Todo, “GIFT: A Small Present,” in Lecture notes in computer science, 2017, pp. 321–345. doi: 10.1007/978-3-319-66787-4_16. Available: https://doi.org/10.1007/978-3-319-66787-4_16

[14] “Review of the NIST Light-Weight Cryptography Finalists,” IEEE Conference Publication | IEEE Xplore, Jun. 01, 2023. Available: https://ieeexplore.ieee.org/document/10257225

[15] H. Madushan, I. Salam, and J. Alawatugoda, “A Review of the NIST Lightweight Cryptography Finalists and Their Fault Analyses,” Electronics, vol. 11, no. 24, p. 4199, Dec. 2022, doi: 10.3390/electronics11244199. Available: https://www.mdpi.com/2079-9292/11/24/4199

[16] “Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities,” IEEE Journals & Magazine | IEEE Xplore, 2021. Available: https://ieeexplore.ieee.org/document/9328432

[17] S. S. Dhanda, B. Singh, and P. Jindal, “Lightweight Cryptography: A Solution to Secure IoT,” Wireless Personal Communications, vol. 112, no. 3, pp. 1947–1980, Jan. 2020, doi: 10.1007/s11277-020-07134-3. Available: https://doi.org/10.1007/s11277-020-07134-3

[18] B. Al-Shargabi, O. Sabri, O. A. Aldabbas, and A. Abuarqoub, “A Survey on Lightweight Encryption Methods for IoT-Enabled Healthcare Applications,” IoT, Dec. 2023, doi: 10.1145/3644713.3644839. Available: https://doi.org/10.1145/3644713.3644839

[19] P. Tran and D. C. Nguyen, “Advanced Lightweight Cryptography for Automotive Security: Surveys, Challenges and Solutions,” IoT, pp. 304–311, Jan. 2022, doi: 10.5220/0011109500003194. Available: https://doi.org/10.5220/0011109500003194

[20] “Lightweight Encryption for Smart Home,” IEEE Conference Publication | IEEE Xplore, Aug. 01, 2016. Available:https://ieeexplore.ieee.org/document/7784596

[21] “ECC Based Authentication Scheme for Smart Homes,” IEEE Conference Publication | IEEE Xplore, Sep. 13, 2021. Available: https://ieeexplore.ieee.org/document/9550911

[22] “Lightweight Cryptographic Approach to Address the Security Issues in Intelligent Applications: A Survey,” IEEE Conference Publication | IEEE Xplore, Jan. 05, 2023. Available: https://ieeexplore.ieee.org/document/10053412

[23] “Evaluating the Performance of Ascon Lightweight Authenticated Encryption for AI-Enabled IoT Devices,” IEEE Conference Publication | IEEE Xplore, Dec. 07, 2022. Available: https://ieeexplore.ieee.org/document/1002441

[24] M. El-Hajj, H. Mousawi, and A. Fadlallah, “Analysis of Lightweight Cryptographic Algorithms on IoT Hardware Platform,” Future Internet, vol. 15, no. 2, p. 54, Jan. 2023, doi: 10.3390/fi15020054. Available: https://www.mdpi.com/1999-5903/15/2/54

[25] S. Pandey and B. Bhushan, “Recent Lightweight cryptography (LWC) based security advances for resource-constrained IoT networks,” Wireless Networks, vol. 30, no. 4, pp. 2987–3026, Mar. 2024, doi: 10.1007/s11276-024-03714-4. Available: https://doi.org/10.1007/s11276-024-03714-4

[26] S. Gupta and S. Saxena, “Lightweight Cryptographic Techniques and Protocols for IoT,” in Transactions on computer systems and networks, 2022, pp. 55–77. doi: 10.1007/978-981-19-1585-7_4. Available: https://doi.org/10.1007/978-981-19-1585-7_4

[27] M. Abu-Tair et al., “Towards Secure and Privacy-Preserving IoT Enabled Smart Home: Architecture and Experimental Study,” Sensors, vol. 20, no. 21, p. 6131, Oct. 2020, doi: 10.3390/s20216131. Available: https://www.mdpi.com/1424-8220/20/21/6131

[28] M. Joshi, B. Mazumdar, and S. Dey, “Lightweight Security Protocols for Securing IoT Devices in Smart Cities,” in Advanced sciences and technologies for security applications, 2021, pp. 89–108. doi: 10.1007/978-3-030-72139-8_5. Available: https://doi.org/10.1007/978-3-030-72139-8_5

[29] “Current Lightweight Cryptography Protocols in Smart City IoT Networks: A Survey,” Arxiv. Available: https://arxiv.org/pdf/2010.00852

[30] Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce, “Lightweight Cryptography | CSRC | CSRC.” Available: https://csrc.nist.gov/Projects/Lightweight-Cryptography

[31] H. Yoshikawa, M. Kaminaga, A. Shikoda and T. Suzuki, "Secret key reconstruction method using round addition dfa on lightweight block cipher lblock", Proc. Int. Symp. Inf. Theory Appl., pp. 493-496

[32] K. Jeong, H. Kang, C. Lee, J. Sung and S. Hong, "First experimental result of power analysis attacks on a FPGA implementation of LEA", Proc. IACR, pp. 621

[33] M. Walter, S. Bulygin and J. Buchmann, "Optimizing guessing strategies for algebraic cryptanalysis with applications to EPCBC", Proc. 8th Int. Conf. Inf. Secur. Cryptol, pp. 175-197, Nov. 2012, [online] Available: https://link.springer.com/chapter/10.1007/978-3-642-38519-3_12.

[34] L. Wen, M. Wang, A. Bogdanov and H. Chen, "Multidimensional zero-correlation attacks on lightweight block cipher HIGHT: Improved cryptanalysis of an ISO standard", Inf. Process. Lett., vol. 114, no. 6, pp. 322-330

[35] C. G. Thorat and V. S. Inamdar, "Implementation of new hybrid lightweight cryptosystem", Appl. Comput. Informat., vol. 16, no. 1, pp. 195-206

[36] E. Oswald, J. Howe, University of Klagenfurt, and University of Bristol, Side Channels: Attacks, Defences, and Evaluation Schemes. pp. 1–15. Available: https://csrc.nist.gov/csrc/media/Presentations/2021/crypto-club-2021-side-channels-1/images-media/crclub-2021-side-channels-1.pdf

[37] S. Jin, M. Xu, and Y. Cai, “Energy Efficient Obfuscation of Side-Channel Leakage for Preventing Side-Channel Attacks,” arXiv.org, Aug. 19, 2022. Available: https://arxiv.org/abs/2208.09140